Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1.   (Currently amended) A method for providing secure message services comprising:

receiving a message including message content for delivery to a recipient;

~~checking for~~ determining preferences for delivery of the message content including security preferences; and

delivering the message content in accordance with the preferences, including securing the message content in accordance with the determined security preferences.

2.   (Previously Presented) The method of claim 1 wherein the preferences are recipient preferences.

3.   (Previously Presented) The method of claim 1 wherein the preferences are sender preferences.

4.   (Previously Presented) The method of claim 1 further comprising receiving the message for delivery to a recipient at a forwarding service.

5.   (Previously Presented) The method of claim 1 wherein the received message is an Email message.

6.   (Previously Presented) The method of claim 1 wherein the received message is an SMTP post.

7.   (Previously Presented) The method of claim 1 wherein the step of delivering the message content includes sending an Email including the message content to the recipient.

8.   (Previously Presented) The method of claim 1 wherein the preferences are preferences associated with a recipient's computer network.

9.   (Previously Presented) The method of claim 1 wherein the preferences are preferences associated with a sender's computer network.

10.   (Previously Presented) The method of claim 1 wherein the recipient is a computer.

11.   (Previously Presented) The method of claim 1 wherein the preferences are set by an administrator of a network associated with one of the sender and the recipient.

12.   (Previously Presented) The method of claim 1 further comprising
        determining if no delivery preference is specified or if Web-based delivery is specified and providing a notification to the recipient including a secure link to the message content.

13.   (Previously Presented) The method of claim 12 wherein the step of providing a notification includes providing an Email to the recipient.

14.   (Previously Presented) The method of claim 1 wherein the step of determining security preferences includes determining a security protocol for use in sending the message

content to the recipient and where the method further includes searching for keys associated with the recipient to be used in encrypting the message content to be sent to the recipient.

15.   (Previously Presented) The method of claim 14 further comprising determining if the located keys can be used in accordance with the determined security protocol, and if so, then securing the message content in accordance with the determined security protocol and using the located keys.

16.   (Previously Presented) A system for securely processing messages for delivery from a sender to a recipient comprising:

a receiving engine for receiving messages from a sender for delivery to a recipient;

a processing engine for processing received messages and for producing standard form messages for selected ones of the messages received from the sender;

a preference engine for determining delivery preferences for the message including security preferences; and

a forwarding engine for forwarding a notification to the recipient if required by the determined delivery preferences, the notification indicating to the user that a message is available to be retrieved;

wherein the processing engine is operable to not produce a standard form message and the forwarding engine is operable to not forward a notification if

the determined preferences indicate direct delivery to the recipient is requested, and

where the security preferences indicate a security protocol by which the message can be securely delivered.

17.   (Previously Presented) The system of claim 16 wherein the selected ones are messages in a non-native format.

18.   (Previously Presented) The system of claim 16 further comprising a storage means for storing standard form messages that are to be temporarily stored in the system.

19.   (Previously Presented) The system of claim 16 wherein the standard form message includes an authentication block, a message block and attachments if any.

20.   (Previously Presented) The system of claim 16 wherein the processing engine is operable to determine an authentication of the sender to use the system.

21.   (Previously Presented) The system of claim 20 wherein the processing engine is operable to determine an authentication of the sender including determining a sender authorization pass phrase for the sender, compare the determined sender authorization pass phrase for the sender with a pass phrased provided by the sender with the message and not forward messages from unauthenticated senders.

22.   (Previously Presented) The system of claim 16 wherein the processing engine includes plural filter layers for processing different types of received messages, one or more of the filter layers providing output of the standard form.

23.   (Previously Presented) The system of claim 16 wherein the preference engine is operable to determine security preferences for the recipient including locating keys associated with the recipient for use in encrypting messages, determining if the keys can be used in accordance with a determined security protocol and sending the message directly to the recipient in accordance with the determined security protocol and using the located keys.

24.   (Currently Amended) A method for providing secure message services using a forwarding service comprising:

receiving a message for delivery to a recipient;

~~checking for~~ determining preferences for delivery of the message content including a security preference where the security preference includes an encryption preference;

if a preference for delivery is specified, delivering the message content in accordance with the delivery preference including encrypting the message content in accordance with the encryption preference.

25. (Previously Presented) The method of claim 24 wherein the step of receiving the message includes receiving an email message.

26. (Previously Presented) The method of claim 24 wherein the step of receiving the message includes receiving an SMTP post that includes the message content.

27. (Previously Presented) The method of claim 24 wherein the step of providing a notification includes providing an email notification.

28. (Previously Presented) The method of claim 24 further comprising storing the message content at least temporarily in a storage means.

29. (Previously Presented) The method of claim 24 further comprising if no preference for delivery is specified, providing a notification to the recipient including a secure link to the stored message content.

30. (Previously Presented) The method of claim 24 further comprising if no preference for delivery and if Web-based delivery is specified, providing a notification to the recipient including a secure link to the stored message content.

31. (Previously Presented) The method of claim 29 or 30 wherein the notification is an email.

32. (Previously Presented) The method of claim 24 wherein the preferences are recipient preferences.

33. (Previously Presented) The method of claim 24 wherein the preferences are sender preferences.

34. (Previously Presented) The method of claim 24 wherein the preferences are preferences associated with a recipient's computer network.

35. (Previously Presented) The method of claim 24 wherein the preferences are preferences associated with a sender's computer network.

36. (Previously Presented) The method of claim 24 wherein the recipient is a computer.

37. (Previously Presented) The method of claim 24 wherein the preferences are set by an administrator of a network associated with one of the sender and the recipient.

38. (Previously Presented) The method of claim 24 wherein the step of determining security preferences includes determining a security protocol for use in sending the message content to the recipient and where the method further includes searching for keys associated with the recipient to be used in encrypting the message content to be sent to the recipient.

39. (Previously Presented) The method of claim 38 further comprising determining if the located keys can be used in accordance with the determined security protocol, and if so, then

securing the message content in accordance with the determined security protocol and using the located keys.

40.   (Previously Presented) The method of claim 24 further comprising producing a standard format message.

41.   (Previously Presented) The method of claim 24 further comprising storing a standard format message in a queue structure.

42.   (Previously Presented) The method of claim 24 further comprising listing user preference data in an access list.

43.   (Previously Presented) A system for securely processing messages for delivery from a sender to a recipient comprising:

receiving means for receiving messages from a sender for delivery to a recipient;

a processing engine for processing received messages for producing standard form messages for at least some of the messages received from the sender;

a delivery engine for determining delivery preferences for a message including security preferences; and

a forwarding engine for forwarding a notification to the recipient if required by the determined delivery preferences, the notification indicating to the user that a message is available to be retrieved.

44.   (Previously Presented) The system of claim 43 wherein one or more of the received messages are email messages.

45.   (Previously Presented) The system of claim 43 wherein one or more of the received messages are SMTP posts that include a message.

46. (Previously Presented) The system of claim 43 wherein the notification is an email notification.

47. (Previously Presented) The system of claim 43 further comprising storage for storing the message at least temporarily.

48. (Previously Presented) The system of claim 43 wherein if the delivery engine determines there is no preference for delivery, the delivery engine provides a notification to the recipient including a secure link to the stored message.

49. (Previously Presented) The system of claim 43 wherein if the delivery engine determines there is no preference for delivery and if Web-based delivery is specified, the delivery engine further providing a notification to the recipient including a secure link to the stored message.

50. (Previously Presented) The system of claims 48 and 49 wherein the notification is an email.

51. (Previously Presented) The system of claim 43 wherein the preferences are recipient preferences.

52. (Previously Presented) The system of claim 43 wherein the preferences are sender preferences.

53. (Previously Presented) The system of claim 43 wherein the preferences are preferences associated with a recipient's computer network.

54. (Previously Presented) The system of claim 43 wherein the preferences are preferences associated with a sender's computer network.

55. (Previously Presented) The system of claim 43 wherein the recipient is a computer.

56. (Previously Presented) The system of claim 43 wherein the preferences are set by an administrator of a network associated with one of the sender and the recipient.

57. (Previously Presented) The system of claim 43 wherein the delivery engine determines a security protocol for use in sending the message to the recipient and searches for keys associated with the recipient to be used in encrypting the message to be sent to the recipient.

58. (Previously Presented) The system of claim 57 wherein the delivery engine determines if the located keys can be used in accordance with the determined security protocol, and if so, then the delivery engine secures the message in accordance with the determined security protocol and uses the located keys.

59. (Previously Presented) The system of claim 43 wherein the delivery engine produces a standard format message.

60. (Previously Presented) The system of claim 59 further comprising a queue structure for storing the standard format message.

61. (Previously Presented) The system of claim 60 wherein the delivery engine is operable to bypass storing the standard form of a message in the queue structure and forward a notification if the determined preferences indicate direct delivery to the recipient is requested, and

where the security preferences indicate a security protocol by which the message can be securely delivered.

62. (Previously Presented) The system of claim 59 wherein the standard form message includes an authentication block, a message block and attachments if any.

63. (Previously Presented) The system of claim 43 wherein the processing engine is operable to determine an authentication of the sender to use the system.

64. (Previously Presented) The system of claim 43 wherein the processing engine is operable to determine an authentication of the sender including determining a sender authorization pass phrase for the sender, compare the determined sender authorization pass phrase for the sender with a pass phrased provided by the sender with the message and not forward messages from unauthenticated senders.

65. (Previously Presented) The system of claim 43 wherein the processing engine includes plural filter layers for processing different types of received messages

66. (Previously Presented) The system of claim 65 wherein each filter layer provides output of a standard format.

67. (Previously Presented) The system of claim 43 wherein the delivery engine is operable to determine security preferences for the recipient including locating keys associated with the recipient for use in encrypting messages, determine if the keys can be used in accordance with a determined security protocol and send the message directly to the recipient in accordance with the determined security protocol and use the located keys.

68.   (New) The method of claim 1, wherein:

determining preferences for delivery of the message content includes determining if a published key is associated with the recipient.

69.   (New) The method of claim 68, wherein:

delivering the message includes encrypting the message if a published key isassociated with the recipient; and

delivering the encrypted message to the recipient.

70.   (New) The method of claim 1, wherein:

determining preferences for delivery of the message content includes determining that no delivery preference is defined; and

delivering the message includes notifying the recipient that the message is available for retrieval.

71.   (New) The method of claim 70, wherein:

delivering the message includes providing a secure link to the message content.

72.   (New) The method of claim 70, wherein:

receiving a message includes receiving an Email message; and

notifying the recipient includes sending an Email notification to the recipient.

73.   (New) The method of claim 1, wherein:

determining preferences for delivery of the message content includes determining if a certificate is associated with the recipient.

74.   (New) The method of claim 1, wherein:

receiving the message includes receiving an Email message.

75.   (New) A computing system for providing secure message services, comprising:
a forwarding engine executing on a computer operable to:

receive a message including message content for delivery to a recipient;

determine recipient preferences for delivery of the message content, including
determining if the recipient has a published key;

if the recipient does not have a published key, notify the recipient that the
message is available for retrieval; and

if the recipient has a published key, encrypt the message and deliver the encrypted
message to the recipient.

76.   (New) The computing system of claim 75, wherein the forwarding engine is
operable to store the message at least temporarily in a storage means.

77.   (New) The computing system of claim 75, wherein the forwarding engine is
operable to provide a secure link to the message content if the recipient does not have a
published key.

78.   (New) A computing system for providing secure message services, comprising:
a forwarding engine executing on a computer operable to:

receive a message including message content for delivery to a recipient;

determine recipient preferences for delivery of the message content, including
determining if a certificate is associated with the recipient;

if a certificate is not associated with the recipient, notify the recipient that the
message is available for retrieval; and

if a certificate is associated with the recipient, encrypt the message and deliver the
encrypted message to the recipient.

79.   (New) The computing system of claim 78, wherein the forwarding engine is operable to store the message at least temporarily in a storage means.

80.   (New) The computing system of claim 78, wherein the forwarding engine is operable to provide a secure link to the message content if a certificate is not associated with the recipient.

81.   (New) A computer implemented method for providing secure message services using a forwarding engine executing on a computer comprising:

       receiving a message including message content for delivery to a recipient;

       determining preferences for delivery of the message content including determining whether there the recipient has a published key;

       if the recipient does not have a published key, notifying the recipient that the message is available for retrieval; and

       if the recipient has a published key, encrypting the message and delivering the encrypted message to the recipient.

82.   (New) The computer implemented method of claim 81, further comprising: storing the message at least temporarily in a storage means.

83.   (New) The computer implemented method of claim 81, wherein if the recipient does not have a published key, the method further comprises:

       providing a secure link to the message content.

84.   (New) A computer implemented method for providing secure message services using a forwarding engine executing on a computer comprising:

       receiving a message including message content for delivery to a recipient;

determining preferences for delivery of the message content including determining if a certificate is associated with the recipient;

if no certificate is associated with the recipient, notifying the recipient that the message is available for retrieval; and

if a certificate is associated with the recipient, encrypting the message and delivering the encrypted message to the recipient.

85. (New) A computer implemented method of claim 84, further comprising:

storing the message at least temporarily in a storage means.

86. (New) A computer implemented method of claim 84, wherein if no certificate is associated with the recipient the method further comprises:

providing a secure link to the message content.

87. (New) A computer program product embodied on an information carrier for providing secure message services using a forwarding engine, the computer program product comprising instructions operable to cause a computer system to:

receive a message including message content for delivery to a recipient;

determine preferences for delivery of the message content, wherein the instructions cause the computer system to determine if the recipient has a published key;

if the recipient does not have a published key, notify the recipient that the message is available for retrieval; and

if the recipient has a published key, encrypt the message and deliver the encrypted message to the recipient.

88. (New) The computer program product of claim 87, further comprising instructions operable to cause a computer system to:

store the message at least temporarily in a storage means.

89.　(New)　The computer program product of claim 87, further comprising instructions operable to cause a computer system to:

provide a secure link to the message content if the recipient does not have a published key.

90.　(New)　A computer program product embodied on an information carrier for providing secure message services using a forwarding engine, the computer program product comprising instructions operable to cause a computer system to:

receive a message including message content for delivery to a recipient;

determine recipient preferences for delivery of the message content, including determining whether a certificate is associated with the recipient;

if there is no certificate associated with the recipient, notify the recipient that the message is available for retrieval; and

if there is a certificate associated with the recipient, encrypt the message and deliver the encrypted message to the recipient.

91.　(New)　The computer program product of claim 90, further comprising instructions operable to cause a computer system to:

store the message at least temporarily in a storage means.

92.　(New)　The computer program product of claim 90, further comprising instructions operable to cause a computer system to:

provide a secure link to the message content.

93.　(New)　A computer implemented method for sending a secure message to multiple recipients comprising:

encrypting a message;

sending the encrypted message to a forwarding server, including providing a list of recipients to the forwarding server;

at the forwarding server, decrypting the message and determining a delivery preference for each recipient in the list of recipients;

for each recipient that has a delivery preference, re-encrypting the message and delivering the message in accordance with the delivery preference; and

for each recipient that does not have a delivery preference, notifying the recipient that the message is available for retrieval.

94. (New) The computer implemented method of claim 93, wherein:

notifying the recipient includes notifying the recipient that the message is available for retrieval through a secure link.

95. (New) The method of claim 93, wherein:

determining a delivery preference for each recipient includes determining whether each recipient has an associated published key.

96. (New) The method of claim 93, wherein:

determining a delivery preference for each recipient includes determining whether each recipient has an associated certificate.

97. (New) A computing system for providing secure message services for messages addressed to multiple recipients, comprising:

a forwarding engine executing on a computer operable to:

receive an encrypted message and a list of recipients;

decrypt the message;

determine a delivery preference for each recipient in the list of recipients;

for each recipient that has a delivery preference, re-encrypt the message and delivering the message in accordance with the delivery preference; and

for each recipient that does not have a delivery preference, notify the recipient that the message is available for retrieval.

98. (New) The forwarding engine of claim 97, wherein the forwarding engine is operable to:

notify the recipient that the message is available for retrieval through a secure link.